Attachment I

Safeguarding Personally Identifiable Information

Background:

The Office of Management and Budget (OMB) memorandum, M-06-15 on "Safeguarding Personally Identifiable Information" dated May 22, 2006, (http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf), reemphasizes Government agency special duties to protect personally identifiable information from loss and misuse.

The Privacy Act, E-Government Act, Federal Information Security Management Act (FISMA), Federal Records Act and Freedom of Information Act and Departmental guidelines for implementing these statutes and OMB directives provide a policy framework that identifies how information must be used and ways to safeguard that information. Attachment I is a listing of the Government and Departmental policy framework which must be followed in these areas.

Penalties:

Noncompliance with Government information safeguard and use requirements is a serious offense. Knowing your role and responsibility in implementing these controls is necessary to avoid Departmental penalties for offenses that concern the mismanagement of information; civil and statutory penalties allowed by the Privacy Act (5 U.S.C. 552a(g) and (i); and those provided in 18 U.S.C. 2071.

1. The Privacy Act includes civil and criminal penalties for violating certain requirements of the Act. A civil remedy applies to the Agency when the plaintiff shows that:
    a. There was a violation of the Privacy Act;
    b. They suffered an adverse effect as a result of the violation;
    c. The agency was a direct or proximate cause of the effect; and
    d. The violation was intentional and willful.

2. A criminal remedy applies to the individual employee and allows for fines up to $5000 for these circumstances:
    a. If an officer or employee of an agency knowingly releases records improperly to a person or agency not entitled to receive it;
    b. If any officer or employee willfully maintains a Privacy Act system without publishing a notice in the Federal Register; and
    c. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses.

3. There are penalties identified for concealment, removal, or mutilation of Federal records which may lead to fines, imprisonment, forfeiting an office and be disqualified from holding office (18 U.S.C.§ 2071).

4. Mismanagement of information and records will not be tolerated at the Department. The Department now has internal corrective procedures for violations addressed in the Department of the Interior Human Resource Manual Section 370 DM 752 on "Discipline and Adverse Actions. Appendix B (the "Table of Offenses and Penalties") identifies several offenses regarding information for which corrective action can be taken against an employee.

Item #2 addresses penalties for: "Improper or unauthorized release of sensitive and administratively-controlled information or employee records; failure to safeguard classified material when: information is not compromised and release is unintentional; information is compromised and release is unintentional; and release of restricted information is deliberate."

Item #12 addresses penalties for: "Loss, misuse of, damage to or failure to safeguard Government property, records, or information (e.g., willful or negligent damage to Government resources; carelessness in performance of duty resulting in waste of public funds)."

5. Executive Performance Element IV: Meeting Other Management Objectives, Section A, addresses protection of information and states: "Ensure that the organization's records, in all formats, are identified, protected, and managed in accordance with Federal and Departmental policies."

Reporting Violations:

Users of information technology resources are responsible for reporting security incidents immediately (375 DM 19.8.N(11) and adhering to National Information Standards and Technology Special Publication 800-53. Each bureau or office has a Computer Security Incident Response Capability (CSIRC) as outlined by 375 DM 19. This CSIRC coordinates with the DOI CSIRC and includes a process for alerting DOI components of an incident, reporting the incident to the DOI CIO, CSIRC, and FedCIRC, and for responding to the incident. DOI CSIRC will share this information with other DOI components, Federal agencies, and organizations.

For paper records, and records in other formats, persons who have identified or suspect a violation of the Privacy Act should follow procedures identified in 370 DM 752, and delegation of authority manual sections. Communicate with Privacy Officers for the above when appropriate.

Actions:

OMB Memorandum M-06-15 requires a review of the Department's policy a

procedures to ensure that adequate safeguards are in place. Please take the following actions and report the necessary information by memorandum by August 18, 2006. Any weaknesses identified must be included in security plans of action and milestones already required by FISMA.

1. Being able to identify systems that maintain personally identifiable information within the organization is the first step in ensuring that appropriate requirements are in place for them.

Each office responsible for the collection, maintenance and use of this information must complete the checklist in Attachment II to evaluate whether appropriate safeguards and maintenance requirements are in place for each Privacy Act system of records. These evaluations must be completed on all Privacy Act systems for which your organization is responsible (see list in Attachment III by bureau/office), and for any grouping of information with personally identifiable information which will include systems that are common throughout the Department and covered by Government-wide notices (see http://www.doi.gov/ocio/privacy/List_doipa_notices_9.03.htm).

System managers responsible for the administration of these systems must apply the appropriate safeguards required in the checklist to the systems identified above. In addition, please ensure that the checklists are distributed as a guide to those offices at the field level within the organization who maintain the same information. In your August 18 response to this office, indicate whether these evaluations were completed on these systems.

2. There may be some systems that maintain personally identifiable information that may not trigger the Privacy Act and would be listed in Attachment III or Government-wide systems (for example, when paper records are filed by date and not a name or personal identifier). Please identify other groupings of information on individuals that your organization maintains and include them in the template provided for each bureau/office in Attachment III when responding to the memorandum. Checklists should be completed for all systems above.

3. Ensure that special attention is given to required training. The Office of the Chief Information Officer has developed three computer-based-training (CBT) modules on Cyber Security, Records Management and the Privacy Act which all employees must complete. The Cyber Security CBT is already available. The Records Management and Privacy Act CBTs will be available at the end of June. All employees and contractors are required to take this training. Please take steps to ensure that your organization is 100% compliant. Provide the percentage completion for your organization for the three CBTs in your memorandum.

4. Report the date when all contracts that involve the contractor's handling of Privacy Act information will be reviewed to ensure that contracts include the required Privacy Act clauses required by the Federal Acquisition Regulations (FAR) and the Department of the Interior (DIAR) Acquisition regulations. (See FAR 52.224-1 and Privacy Act Notification at FAR 24.104(a), supplemental information at DIAR 1452.224-1, and 43 CFR 2.53).

5. Report the date when a review would be completed of contracts that generate records as a result of contractual obligations and that are properly identified and included in the agency's official recordkeeping system. Notify Bureau Records Officers of this.

6. Report the date when MOUs , data sharing agreements, and other agreements will be reviewed to ensure that they address roles and responsibilities for implementing information management requirements (privacy, security, FOIA, records, etc.). Often these responsibilities are not included and are essential to ensure compliance with Government laws and guidelines.

7. Report that a review of bureau/office telework policy was done to ensure it is consistent with that issued by Personnel Bulletin No. 05-02 on February 18, 2005. Special attention should be given to sections 3.1 Q. on "Security and Liability Issues"; 3.1.S. on "Privacy Act Considerations"; 3.1. U. on "Recordkeeping Requirements"; and compliance with items on records, privacy and security in the telework agreement. Identify the date of when changes will be made to the bureau/office telework policy to ensure they are consistent with the Personnel Bulletin.

Scope:

Safeguard and use requirements apply to all persons who collect, have access to, maintain, use, or make decisions on personal information identifiable to the individual. It applies to any situation such as teleworking or contracting where the information is involved. Reviews will involve program offices collecting information, system managers, Cyber Security Specialists and Privacy Act Officers.

Due Dates:

Please provide by August 18, 2006, a signed memorandum to the Chief Information Officer, Department of the Interior addressing the actions above.

Contact:

Reports should be submitted to the Chief Information Officer, Room 5312 MIB, 1849 C. St. NW, Washington, DC 20240 by the date above. For specific questions on this and the OMB memorandum please have you staff contact Marilyn Legnini, Departmental Privacy Officer (202-219-0868) or marilyn_legnini@ios.doi.gov.